JAMES L. MASSEY

Some Algebraic and Distance Properties of Convolutional Codes

Proc. Symposium on Error Correcting Codes, U. S. Army Research Center, University of Wisconsin, Madison, Wisconsin, May 6-8, 1968 (John Wiley and Sons, Inc., New York, 1968, pp. 89-109)

ABSTRACT

A Plotkin-type upper bound and a Gilbert-type lower bound are proved for the feedback-decoding and definite-decoding minimum distances respectively of binary convolutional codes. In the former case, a very simple bound is derived which shows that the ratio of feedback decoding minimum distance to constraint length is asymptotically upper-bounded by $\frac{1}{2}(1-R)$ for codes of rate R. In the latter case, it is shown that the ratio d_{DD}/n_{DD} of definite-decoding minimum distance to constraint length is asymptotically lower bounded as $H(d_{DD}/n_{DD}) \geq 0.1\,(1-R)/(1+R)$ for the best codes of rate R. This derivation requires the development of several interesting relationships between convolutional codes and linear feedback shift-registers.

1. Introduction

In the following sections, we shall present some bounds on the attainable minimum distance for convolutional codes. The derivation of these bound leads also to the establishment of certain interesting algebraic properties of these codes. The results herein have evolved over the past several years and have benefitted considerably from the work of several of our students, particularly R. Kolor and W. Wilder, to the point that they are now sufficiently unified to offer to other workers in the field. In this section, we review the necessary background material on convolutional codes required in the following sections.

In this paper, only convolutional codes in canonic systematic form will be considered and the reader is referred to the literature [1] for the justification that this results in no loss of generality. For convenience, the discussion will also be restricted to binary codes unless explicitly stated to the contrary.

Let $\underline{i}_u$ denote a K-dimensional column vector over GF(2), the binary number field. Then $\underline{i}_0, \underline{i}_1, \cdots, \underline{i}_u, \cdots$ denotes a sequence

of such vectors and we shall consider that the components of $\underline{i}_u$ are the K information digits to be encoded at time instant u . A (canonic systematic) convolutional code of memory order m is specified by the matrices $G_0, G_1, \ldots, G_m$ where each G_j is an $(N-K)\times K$ binary matrix. The N encoded digits at time instant u are the components of the column vector whose first K components form $\underline{i}_u$ and whose last N-K components form the vector $\underline{p}_u$ given by

$$\underline{p}_u = G_0\underline{i}_u + G_1\underline{i}_{u-1} + \ldots + G_m\underline{i}_{u-m} \qquad (1)$$

where we assume $\underline{i}_j = \underline{0}$ if $j < 0$. The components of $\underline{p}_u$ are the N-K parity digits formed by the convolutional code at time instant u . The rate R of the code is defined as $R = K/N$.

It should be noted from (1) that a convolutional code of memory order $m = 0$ is just a systematic linear block code and conversely. Hence the theory of convolutional codes includes that of block codes as a special case which perhaps accounts for the greater difficulty with which distance bounds are derived for the former class of codes.

2. A Plotkin Upper Bound on Feedback Decoding Minimum Distance

The usual decoding method for convolutional codes, called feedback decoding (FD) by Robinson [2], calls for the decoding estimate of $\underline{i}_u$ to be made from the received digits over time units u through u+m on the assumption that $\underline{i}_{u-1}, \ldots, \underline{i}_{u-m}$ have all been correctly decoded. With this assumption, the decoding of $\underline{i}_0$ is typical of the decoding of any $\underline{i}_u$ and hence the feedback-decoding minimum distance, d_{FD}, is appropriately defined as the fewest number of positions that two encoded sequences with differing values of $\underline{i}_0$ are found to disagree over the time span 0 through m . The total number of positions within this time span, namely $(m+1)N$, is called the feedback-decoding constraint length and will be denoted as n_{FD} . By the usual linearity argument, it follows that

$$d_{FD} = \min_{\underline{i}_0 \neq \underline{0}} W_H(\underline{i}_0, \underline{i}_1, \ldots, \underline{i}_m, \underline{p}_0, \underline{p}_1, \ldots, \underline{p}_m) \qquad (2)$$

where $W_H(\ )$ denotes the Hamming weight, i.e. the number of non-zero components among the vectors, of the enclosed vectors.

In the remainder of this section, an upper bound on the ratio d_{FD}/n_{FD} will be obtained which as n_{FD} increases tends to the same value as the familiar asymptotic Plotkin upper bound for block codes with the same rate R . Hence this bound for convolutional codes will also be called a Plotkin bound. The derivation of this bound is facilitated by the introduction of the following:

Definition 1: The integer $d(m, N, K)$ is the maximum value of d_{FD} for the class of all convolutional codes of memory order m for encoding K binary digits per time instant into N digits.

In terms of the quantity $d(m, N, K)$, we next state four lemmas which will then be combined to yield the sought-for Plotkin bound.

Lemma 1: $d(m, N, K) \leq d(m, N-K+1, 1)$.

Proof: Note that the partial minimization of the righthand side of (2) over those $\underline{i}_u$ which are all zero in their last $K-1$ components is equivalent to the full minimization for the code with 1 information and $N-(K-1)$ encoded digits per time instant whose matrices G_j are just the first columns of the original matrices. Hence, for every code with K information and N encoded digits per time instant there is a code with 1 information and $N-K+1$ encoded digits per time instant whose minimum distance d_{FD} is at least as great as that of the first code.

Lemma 2: For N odd, $d(m, N, 1) \leq N + m\frac{N-1}{2}$.

Proof: We claim first that when $K = 1$, there will be a code having $d_{FD} = d(m, N, K)$ and having $G_0 = (1, 1, \ldots, 1)$ the $(N-1)$-dimensional all-one column vector. To show this, consider first any code in which the k-th component of G_0 is 0 . If this is also true for every G_j, then from (1) it follows that the k-th component of $\underline{p}_u$ is 0 for all u, so that changing the k-th component of G_0 to 1 will increase d_{FD} . Otherwise, let n be the smallest integer such that G_n has a 1 in the k-th component. From (1) it follows that $\underline{p}_u$ has a 0 in its k-th component for $u < n$. From (1) it also follows that moving the k-th component of G_{n+j} to the k-th component of G_j, $j = 0, 1, \ldots (m-n)$, has only the effect of moving the k-th component of $\underline{p}_{n+j}$ to the k-th component of $\underline{p}_j$ for all $j \geq 0$. Hence, we see from (2) that this new code has d_{FD} at least as great as the original code, and we also note that this new code has a 1 in the k-th component of G_0 . Since k is arbitrary, the claim follows.

It remains to show that when $G_0 = (1, 1, \ldots, 1)$ and $i_0 = 1$, then it is always possible to choose $i_1, \ldots, i_m$ to produce a vector $(i_0, i_1, \ldots, i_m, \underline{p}_0, \underline{p}_1, \ldots, \underline{p}_m)$ whose Hamming weight satisfies the inequality in the lemma. Note first that $(i_0, \underline{p}_0) = (1, G_0)$ and hence has weight N . But for any fixed code, any $u > 0$, and any fixed choice of $i_1, i_2, \ldots, i_{u-1}$, it follows from (1) that

$$(i_u, \underline{p}_u) = (i_u, i_u, \ldots, i_u) + (0, \sum_{j=1}^{u} G_j i_{u-j}) \quad .$$

Since the second vector on the right is a fixed N-vector, it follows that the choices $i_u = 0$ and $i_u = 1$ result in N-vectors that are complements of one another for $(i_u, \underline{p}_u)$. But since N is odd, one of

these N vectors must have weight at most $(N-1)/2$. Hence, for any code, we can choose $i_1, i_2, \ldots, i_m$ in order so that $(i_u, \underline{p}_u)$ has weight at most $(N-1)/2$ for $u = 1, 2, \ldots, m$ and the lemma is proved.

Lemma 3: For m even, $d(m, N, K) \leq d(\frac{m}{2}, 2N, 2K)$.

Proof: For any code with parameters $m = 2m^*$, N, K and defining matrices $G_0, G_1, \ldots, G_{2m^*}$ we consider the new code with parameters m^*, $N^* = 2N$ and $K^* = 2K$ with defining matrices

$$G_j^* = \begin{bmatrix} G_{2j} & G_{2j-1} \\ G_{2j+1} & G_{2j} \end{bmatrix} \qquad j = 0, 1, \ldots, m^*$$

where we define G_{-1} and G_{m+1} both to be the all zero matrix. Also, we set the $N^* = 2N$ vector

$$\underline{i}_j^* = (\underline{i}_{2j}, \underline{i}_{2j+1})$$

and set the $N^* - K^* = 2(N-K)$ vector

$$\underline{p}_j^* = (\underline{p}_{2j}, \underline{p}_{2j+1}) .$$

It is then readily checked that for this new code, p_u satisfies (1) with the matrices G_j of the old code. Hence, from (2), it follows that the minimum distance of the new code satisfies

$$d_{FD}^* = \min_{\substack{\underline{i}_0 \neq 0 \text{ or } \underline{i}_1 \neq 0 \\ \text{or both}}} W_H(\underline{i}_0, \underline{i}_1, \ldots, \underline{i}_{m+1}, \underline{p}_0, \underline{p}_1, \ldots, \underline{p}_{m+1})$$

where the righthand side is evaluated for the old code. Hence the minimum clearly occurs with $\underline{i}_0 = \underline{0}$ (which implies $\underline{p}_0 = \underline{0}$) and $\underline{i}_1 \neq \underline{0}$ so that the righthand side of the preceding equation differs from (2) only by a trivial increase in indices by one and hence also has value d_{FD}. Hence, we have shown that for m even, given any code with parameters m, N and K, we can construct a second code with parameters $\frac{m}{2}$, 2N, and 2K having the same minimum distance and thus the lemma is proved.

The last preliminary result which we shall need is the self-evident:

Lemma 4: $d(m, N, K) \leq d(m+1, N, K)$.

We are now in a position to prove the main result of this section.

Theorem 1: $d(m, N, K) \leq \left[\frac{m+5}{2}\right](N-K) + 1$, where the square brackets denote the integer part of the enclosed number.

Proof: Consider first the case when $(N-K)$ is even. Then

$$d(m, N, K) \leq d(m, N-K+1, 1) \leq (N-K+1) + \frac{m}{2}(N-K)$$

where the first inequality follows from lemma 1 and the second from lemma 2. Hence the inequality in the theorem actually holds with strict inequality in this case.

Next consider the case when $(N-K)$ is odd. Then

$$d(m, N, K) \leq d(m, N-K+1, 1) \leq d\left(\left[\frac{m+1}{2}\right], 2N-2K+2, 2\right)$$

where the first inequality follows from lemma 1 and the second from the combination of lemmas 3 and 4. Again applying lemmas 1 and 2 in order to the last member of the preceding inequality, we obtain

$$d(m, N, K) \leq d\left(\left[\frac{m+1}{2}\right], 2N-2K+1, 1\right) \leq 2(N-K) + 1 + \left[\frac{m+1}{2}\right](N-K)$$

which is equivalent to the inequality in the theorem. Thus the theorem is proved for all cases.

Recalling that $n_{FD} = (m+1)N$ and that $R = K/N$, we obtain immediately from Theorem 1:

Corollary 1: $$\lim_{m\to\infty} \frac{d(m, N, K)}{n_{FD}} \leq \frac{1}{2}(1-R) .$$

Corollary 1, which is the asymptotic case of Theorem 1 for large constraint lengths n_{FD}, provides an upper bound for the ratio d_{FD}/n_{FD} that coincides with the usual asymptotic Plotkin upper bound [3] for the d_{min}/n ratio for a block code with rate R and constraint length n.

The key idea in deriving the preceding bound, namely the content of lemma 2, was first pointed out to the author by Jones [4] in 1962. The content of this lemma has also been independently stated by Lin and Lyne [5]. The remainder of the derivation, i.e. the necessary tricks to reduce the general case so that lemma 2 may be applied, was supplied by the author.

Wilder [6] has recently generalized the preceding derivations to convolutional codes defined over an arbitrary finite field $GF(q)$. In this general case, the righthand side of the inequality in corollary 1 becomes $\frac{q-1}{q}(1-R)$ which coincides with the asymptotic Plotkin bound for block codes. More surprisingly, in the binary case, Wilder found that the inequality in lemma 2 is an equality in many instances. For $N = 3$, Bussgang's tabulation [7] of optimal codes shows that equality is obtained for $m \leq 6$. Wilder found equality for $m \leq 4$

when $N = 5$, and equality for $m \leq 3$ for general N. Wilder also succeeded in generalizing lemma 2 to apply to a class of nonlinear tree codes of which convolutional codes are the linear special case.

3. Gilbert Lower Bound on Definite-Decoding Minimum Distance

A. The Gilbert Bound on Feedback-Decoding Minimum Distance

We digress momentarily to consider the well-known Gilbert lower bound on d_{FD}. For clarity, we treat only the case where $N = K + 1$, i.e. where $\underline{p}_u$ is a single binary digit p_u and $R = \frac{K}{K+1}$. In this case, the matrices G_j, which have dimension $(N - K) \times K$ in general, are simply K-dimensional row vectors. We shall emphasize this fact by writing the matrix G_j as $\underline{G}_j$. We shall here and hereafter use a prime to denote the transpose of a vector so that $\underline{G}_j'$ for instance is a K-dimensional column vector. With this notation, it then follows from (1) that

$$\begin{bmatrix} p_0 \\ p_1 \\ \vdots \\ p_m \end{bmatrix} = \begin{bmatrix} \underline{i}_0' & \underline{0}' & \cdots & \underline{0}' \\ \underline{i}_1 & \underline{i}_0' & \cdots & \underline{0}' \\ \vdots & & & \\ \underline{i}_m' & \underline{i}_{m-1}' & \cdots & \underline{i}_0' \end{bmatrix} \begin{bmatrix} \underline{G}_0' \\ \underline{G}_1' \\ \\ \underline{G}_m' \end{bmatrix} \tag{3}$$

and we shall refer to the matrix of information vectors in (3) as the $\underline{i}$-matrix. Note that the $\underline{i}$-matrix is an $(m+1) \times (m+1)K$ dimensional matrix of binary digits. We shall refer to the $(m+1)$-dimensional vector on the lefthand side of (3) as the p-vector, and shall refer to the $(m+1)K$-dimensional vector $(\underline{i}_0, \underline{i}_1, \cdots, \underline{i}_m)$ as the $\underline{i}$-vector.

A particular code will have $d_{FD} < d$ if and only if there is an $\underline{i}$-vector with $\underline{i}_0 \neq \underline{0}$ and a p-vector satisfying (3) whose combined Hamming weight is less than d. But since there are only $n_{FD} = (K+1)(m+1)$ positions in the combined vectors, there are only

$$\sum_{j=0}^{d-1} \binom{n_{FD}}{j} < 2^{n_{FD} H\left(\frac{d}{n_{FD}}\right)} \tag{4}$$

possible choices of low weight combinations. In obtaining (4), use has been made of the well-known inequality [8]

$$\sum_{j=0}^{\delta n} \binom{n}{j} \leq 2^{nH(\delta)} \quad \text{when} \quad \delta \leq \frac{1}{2} \tag{5}$$

where $H(\delta) = -\delta \log_2 \delta - (1-\delta) \log_2 (1-\delta)$ is the binary entropy function. Note next that $\underline{i}_0 \neq \underline{0}$ guarantees that the $\underline{i}$-matrix in (3) has rank exactly $m+1$ so that any combination of an $\underline{i}$-vector with $\underline{i}_0 \neq \underline{0}$ and a p-vector is a solution of (3) for a fraction exactly $2^{-(m+1)}$ of all the codes. Hence, it follows from (4) that if

$$2^{n_{FD} H(\frac{d}{n_{FD}}) - (m+1)} < 1 ,$$

then not all the codes have a combined $\underline{i}$-vector and p-vector with $\underline{i}_0 \neq \underline{0}$ with Hamming weight less than d. Hence it follows that there must exist at least one code such that its minimum distance satisfies

$$2^{n_{FD} H(d_{FD}/n_{FD}) - (m+1)} \geq 1 = 2^0 .$$

Since $(m+1) = n_{FD}(1-R)$, this inequality can be written

$$H(d_{FD}/n_{FD}) \geq 1 - R \qquad (6)$$

for at least one convolutional code of rate R and constraint length n_{FD}. Inequality (6) is the usual asymptotic Gilbert bound [9] which holds for arbitrary $R = K/N$ although the derivation here has been restricted to $N = K+1$.

B. The Gilbert Bound on d_{DD}

A second decoding method for convolutional codes, called <u>definite decoding</u> (DD) by Robinson [2], calls for the decoding estimate of $\underline{i}_u$ to be made without employing previous decoding estimates. The purpose of DD is to avoid the error-propagation effect inherent in feedback decoding. In particular, we assume that the decoding estimate of $\underline{i}_u$ is to be based on the received digits corresponding to $\underline{i}_{u-m}, \underline{i}_{u-m+1}, \cdots, \underline{i}_{u+m}$ and to $\underline{p}_u, \cdots, \underline{p}_{u+m}$, i.e. corresponding to the parity digits affected by $\underline{i}_u$ and to all the information digits affecting these parity digits. The number of these digits is the <u>definite-decoding constraint length</u>, n_{DD}.

$$n_{DD} = (2m+1)K + (m+1)(N-K) .$$

In order to make $u = 0$ typical of the general case, we abrogate our previous assumption that $\underline{i}_u = \underline{0}$ for $u < 0$ and hereafter allow these past information digits to assume arbitrary values. The <u>definite-decoding minimum distance</u>, d_{DD}, is then appropriately defined as the fewest number of positions that two encoded sequences with differing values of $\underline{i}_0$ are found to disagree over the DD constraint length. By the usual linearity argument, it then follows that

$$d_{DD} = \min_{\underline{i}_0 \neq \underline{0}} W_H(\underline{i}_{-m}, \underline{i}_{-m+1}, \cdots, \underline{i}_m, \underline{p}_0, \underline{p}_1, \cdots, \underline{p}_m) \ . \qquad (7)$$

Comparison of (2) and (7) reveals that for any code $d_{DD} \leq d_{FD}$. Hence, upper bounds on d_{FD} are a fortiori upper bounds on d_{DD} , but lower bounds on d_{FD} cannot be presumed to be lower bounds on d_{DD} .

Until further notice, we consider only the case $N = K + 1$ as was done in the preceding subsection. For this case, we have

$$n_{DD} = (2m + 1)K + (m + 1) \qquad (8)$$

and from (3) as modified to account for the fact that we no longer assume $\underline{i}_u = \underline{0}$ for $u < 0$

$$\begin{bmatrix} p_0 \\ p_1 \\ \vdots \\ p_m \end{bmatrix} = \begin{bmatrix} \underline{i}'_0 & \underline{i}'_{-1} & \cdots & \underline{i}'_{-m} \\ \underline{i}'_1 & \underline{i}'_0 & \cdots & \underline{i}_{-m+1} \\ & & \vdots & \\ \underline{i}'_m & \underline{i}'_{m-1} & \cdots & \underline{i}'_0 \end{bmatrix} \begin{bmatrix} \underline{G}'_0 \\ \underline{G}'_1 \\ \vdots \\ \underline{G}'_m \end{bmatrix} \ . \qquad (9)$$

In the remainder of this subsection, we prove a lower bound on d_{DD} which we call a "Gilbert bound" not because of a formal similarity to (6) but because the method of proof will be along the same lines that led to (6). That some modification in the proof will be required is clear from the fact that when $\underline{i}_u = (1, 1, \ldots, 1)$, all u, then the $\underline{i}$-matrix in (9) has rank only 1 and hence fully 2^{-1} or one-half of all the codes have the p-vector $(0, 0, \ldots, 0)$ occuring in combination with this one particular $\underline{i}$-matrix. Fortunately, the combined p-vector and $\underline{i}$-vector [where we now take the $\underline{i}$-vector to be $(\underline{i}_{-m}, \underline{i}_{-m+1}, \ldots, \underline{i}_m)$] have high Hamming weight so that it does not follow that this one-half of the codes have small definite-decoding minimum distance. For ease of reference, the combined $\underline{i}$-vector and p-vector, i.e. the vector

$$(\underline{i}_{-m}, \underline{i}_{-m+1}, \cdots, \underline{i}_m, p_0, p_1, \ldots, p_m) \ ,$$

will be called the code-vector.

The argument that we shall use to obtain the Gilbert lower bound on d_{DD} runs roughly as follows: Let M_r be the number of code-vectors with $\underline{i}_0 \neq \underline{0}$ such that the $\underline{i}$-matrix has rank r and W_H(code-vector) $< d$. Then (assuming that it appears in some code) each such code vector appears in a fraction 2^{-r} of all the codes. Hence if

$$\sum_{r=1}^{m+1} M_r 2^{-r} < 1 ,$$

then there must exist at least one code such that $d_{DD} \geq d$.

1. Periodic $\underline{i}$-Matrices and Linear FSR's

Definition 2: A periodic matrix is a matrix

$$\begin{bmatrix} \underline{a}'_0 & \underline{a}'_{-1} & \cdots & \underline{a}'_{-n} \\ \underline{a}'_1 & \underline{a}'_0 & \cdots & \underline{a}'_{-n+1} \\ \vdots & & & \\ \underline{a}'_m & \underline{a}'_{m-1} & \cdots & \underline{a}'_{m-n} \end{bmatrix} \qquad \begin{matrix} n \geq n \geq r \\ 1 \leq r \leq m \end{matrix} \qquad (10)$$

(where each $\underline{a}_j$ is a K-dimensional binary column vector) such that the matrix has rank r, its first r rows are linearly independent, and the linear combination of the first r rows which produces the (r+1)-st row includes the first row with a multiplier of 1 .

Thus if A_j denotes the (j+1)-st row of a periodic matrix (10), then

$$A_j = \sum_{g=1}^{r} c_g A_{j-g} \quad (c_r = 1) \quad j = r, r+1, \ldots, m . \qquad (11)$$

(11) holds by the definition of a periodic matrix when $j = r$; the form of (10) and the fact that A_j, $j > r$, must be linearly dependent on preceding rows guarantees that (11) must hold for $j > r$ as well. Conversely, if $r > 0$ is the smallest integer such that a recursion of the form (11) holds, then a matrix of the form (10) is periodic with rank r .

We see directly from (10) that (11) is fully equivalent to

$$\underline{a}_j = \sum_{g=1}^{r} c_g \underline{a}_{j-g} \quad (c_r = 1) \quad j = r-n, r-n+1, \ldots, m . \qquad (12)$$

Letting a_{jK+h-1}, $h = 1, 2, \ldots, K$, denote the h-th digit in $\underline{a}_j$, we see that (12) in turn is fully equivalent to

$$a_j = \sum_{g=1}^{r} c_g a_{j-gK} \quad (c_r = 1) \quad j = (r-n)K, (r-n)K+1, \ldots, mK+K-1 . \qquad (13)$$

We define the outer-fringe of a periodic matrix (10) to be the vector

$$(\underline{a}_{-n}, \underline{a}_{-n+1}, \cdots, \underline{a}_{m}) = (a_{-nK}, a_{-nK+1}, \cdots, a_{mK+K-1})$$

and note that this is an $(m+n+1)K$-dimensional column vector. The recursion (13) is just the statement that the outer-fringe is an $(m+n+1)K$ digit output segment of a linear feedback shift-register (FSR) with tap connections every K-th stage as determined by $c_1, c_2, \ldots, c_r$. This FSR is shown in Figure 1. Note that since $c_r = 1$, the last stage of this rK-stage linear FSR is always tapped, i.e. the FSR is non-singular, and it is well-known in this case that all output sequences are periodic. This is the motivation for the nomenclature in definition 2, although of course the outer-fringe may not contain a complete period of an output sequence since the latter can in fact be as great as $K(2^r - 1)$. We note further that the outer-fringe cannot be an output segment of any such FSR with fewer than rK stages since in the latter case the periodic matrix (10) would be found to have rank less than r. We state the essential facts brought out in this discussion as:

Theorem 2: The outer-fringe of a rank r periodic matrix (10) is an $(m+n+1)K > 2rK$ digit output segment of a unique rK-stage nonsingular linear FSR and of no shorter linear FSR tapped only every K-th stage.

We next turn our attention to proving several facts about the output sequences of FSR's that will be exploited in the sequel. It will prove convenient to state these results in terms of the fractional weight of a vector $\underline{v}$ which we define to be the quantity $\frac{1}{n} W_H(\underline{v})$ where n is the dimension of $\underline{v}$.

Lemma 5: For any $n \geq L > 0$, and any δ, $0 < \delta \leq \frac{1}{2}$, the number of binary n-digit segments in any set such that each segment has fractional weight δ or less and no two segments coincide in any span of L consecutive digits is less than $2^{3LH(\delta)}$.

Proof: Let M be the maximum number of segments in such a set and suppose first that $L \leq n < 3L$. Since all segments must be distinct

$$M \leq \sum_{j=0}^{[\delta n]} \binom{n}{j} < \sum_{j=0}^{[3\delta L]} \binom{3L}{j} \leq 2^{3LH(\delta)}$$

where we have made use of (5) and [ ] throughout this proof denotes the integer part of the enclosed number. It remains to consider $n \geq 3L$. Let $n = iL + n'$ where i is the quotient and n' the remainder when n is divided by L. We note that no segment can have weight more than $[\delta n]$ and hence each segment must have weight $[\frac{4}{3}\delta iL]$ or less in its first iL positions. Suppose that

$$M \geq \sum_{j=0}^{m} \binom{L}{j} = M' \quad \text{where} \quad m = [\tfrac{8}{3}\delta L + 1] \ .$$

In each of the first i spans of L digits, the average weight of the M segments cannot be less than that of the M' distinct lowest weight vectors of length L, i.e. the $\binom{L}{j}$ vectors of weight j for $j = 0, 1, \ldots, m$. But, for any $k < \frac{1}{2}m$, the $\binom{L}{k}$ vectors of weight k are outnumbered by the $\binom{L}{m-k}$ vectors of weight $m-k$ so that the average weight of these M' vectors exceeds $\frac{1}{2}m$. Hence, in their first iL digits, the M segments have average weight exceeding $\frac{1}{2}m = \frac{1}{2}[\frac{8}{3}\delta L + 1] \geq [\frac{4}{3}\delta iL]$ contradicting the fact none has weight more than $[\frac{4}{3}\delta iL]$ over this span of iL digits. Hence we conclude that

$$M < \sum_{j=0}^{[\frac{8}{3}\delta L + 1]} \binom{L}{j} \leq 2^{LH\left(\frac{[\frac{8}{3}\delta L + 1]}{L}\right)} \leq 2^{LH(3\delta)} \leq 2^{3LH(\delta)} \ ,$$

where the third inequality holds under the further proviso that $\delta L \geq \frac{2}{3}$ since $[\frac{8}{3}x + 1] \leq 3x$ for any $x \geq \frac{2}{3}$. The remaining case where $\delta < \frac{2}{3L}$ is trivial and it is readily checked that the lemma is true in this case.

An immediate application of lemma 5 yields:

Lemma 6: For any $n \geq L$, and any δ, $0 < \delta \leq \frac{1}{2}$, of the 2^L distinct output segments of length n obtainable from an L-stage nonsingular linear FSR, fewer than $2^{3LH(\delta)}$ have fractional weight δ or less.

Proof: We simply note that any L consecutive digits in an output segment determine a state of the FSR (see Figure 1 which is the special case of an $L = rK$ stage register) so that any two segments which agree in such a span must agree everywhere thereafter. But since the output sequences of the FSR are periodic, the segments must also agree in their previous digits and hence must be the same segment. The lemma now follows directly from lemma 5.

Lemma 7: Given fixed values of m, n, K and r in definition 2, the number of distinct outer-fringes of rank r periodic matrices such that the outer-fringe has fractional weight δ or less, $0 < \delta \leq \frac{1}{2}$, is less than $2^{6KrH(\delta)}$.

Proof: It can be shown [10] that if the shortest linear FSR which can generate an n-digit, $n \geq 2L$, segment has length L, then any $2L$ successive digits in the segment uniquely determine the FSR. Hence, from theorem 2, we conclude that any $2Kr$ successive digits in the outer-fringe uniquely determine the entire outer-fringe. Thus there

can be no more valid outer-fringes of fractional weight δ or less than there are $(m+n+1)K > 2rK$ digit segments of fractional weight δ or less such that no two coincide in any $2rK$ consecutive positions. By lemma 5, this number is less than $2^{3(2rK)H(\delta)} = 2^{6rKH(\delta)}$

We are now prepared to connect the notion of a periodic matrix with the $\underline{i}$ matrix in (9).

Theorem 3: If the $\underline{i}$-matrix in (9) has rank $r < \frac{m}{3}$, then the reduced $\underline{i}$-matrix

$$\begin{bmatrix} \underline{i}'_r & \underline{i}'_{r-1} & \cdots & \underline{i}'_{r-m} \\ \underline{i}'_{r+1} & \underline{i}'_r & \cdots & \underline{i}'_{r-m+1} \\ \vdots & & & \\ \underline{i}'_{m-r} & \underline{i}'_{m-r-1} & \cdots & \underline{i}'_{-r} \end{bmatrix} \tag{14}$$

is a periodic matrix of rank L, $L \leq r$, whenever $\underline{i}_0 \neq \underline{0}$.

Proof: Let I_j denote the $(j+1)$-st row in the i-matrix of (9) and let s be the least index such that I_s is a linear combination of preceding rows. Let I_{s-L} be the first row appearing with multiplier 1 in the unique combination of the first s rows which forms I_s, then

$$I_s = \sum_{g=1}^{L} c_g I_{s-g} \quad (c_L = 1) \tag{15}$$

and we note that $L \leq s \leq r$. If $r = s$, all rows after I_s must also satisfy the recursion (15) and hence the theorem is trivially true. If not, suppose that $t > s$ is the least index such that (15) is not satisfied, i.e.

$$I_j = \sum_{g=1}^{L} c_g I_{j-g} \quad (c_L = 1) \quad j = s, s+1, \ldots, t-1 \tag{16}$$

but

$$I_t \neq \sum_{g=1}^{L} c_g I_{t-g} \quad (c_L = 1) \ . \tag{17}$$

In this case, we claim that the $\underline{i}$-matrix in (9) has rank exactly $(m+1) + (t-s)$. To show this, note that (16) and (17) are equivalent to

$$\underline{i}_j = \sum_{g=1}^{L} c_g \underline{i}_{j-g} \qquad j = s-m, s-m+1, \ldots, t-1 \tag{18}$$

and

$$\underline{i}_t \neq \sum_{g=1}^{L} c_g \underline{i}_{t-g} \ . \tag{19}$$

Now suppose that I_u, for any $u \geq t$, can be written as a linear combination of preceding rows, i.e.

$$I_u = \sum_{h=1}^{u} a_h I_{u-h} \ . \tag{20}$$

But (20) is equivalent to

$$\underline{i}_j = \sum_{h=1}^{u} a_h \underline{i}_{j-h} \qquad j = u-m, u-m+1, \ldots, u \tag{20'}$$

which in particular, since $u-m < t \leq u$, implies

$$\underline{i}_t = \sum_{h=1}^{u} a_h \underline{i}_{t-h} \ . \tag{21}$$

But the terms in the summation on the righthand side of (21) involve only $\underline{i}_j$ for j in the range such that (18) is valid. Hence we may use (18) in (21) to obtain

$$\underline{i}_t = \sum_{h=1}^{u} a_h \sum_{g=1}^{L} c_g \underline{i}_{t-h-g} = \sum_{g=1}^{L} c_g \sum_{h=1}^{u} a_h \underline{i}_{t-g-h} \ . \tag{22}$$

We now recognize, since $t-u-L > u-m$, that (20') may be used to rewrite the righthand side of (22) which yields

$$\underline{i}_t = \sum_{g=1}^{L} c_g \underline{i}_{t-g} \tag{23}$$

and hence gives a contradiction of (19). We conclude that the only rows in the $\underline{i}$-matrix (9) which can be written as linear combinations of preceding rows are the $t-s$ rows satisfying (16). Since the matrix has $m+1$ rows, its rank then is exacly $(m+1) - (t-s)$ as

claimed. But the rank r is given as less than $\frac{m}{3}$. We have already noted that $s \leq r$, and hence $t = (m+1) - r + s > m - r$. Hence all the rows in the reduced $\underline{i}$-matrix (14) are rows which satisfy the recursion (16) and hence this $\underline{i}$-matrix is periodic as claimed. Moreover it has rank $L \leq r$.

From (9), we find that

$$\begin{bmatrix} p_r \\ p_{r+1} \\ \vdots \\ p_{m-r} \end{bmatrix} = \begin{bmatrix} \underline{i}'_r & \underline{i}'_{r-1} & \cdots & \underline{i}'_{r-m} \\ \underline{i}'_{r+1} & \underline{i}'_r & \cdots & \underline{i}'_{r-m+1} \\ & & \vdots & \\ \underline{i}'_{m-r} & \underline{i}'_{m-r-1} & \cdots & \underline{i}'_{-r} \end{bmatrix} \begin{bmatrix} \underline{G}'_0 \\ \underline{G}'_1 \\ \vdots \\ \underline{G}'_m \end{bmatrix} . \tag{24}$$

We call the lefthand side of (24) the reduced p-vector and note that it is $m - 2r + 1$ component vector uniquely determined by the reduced $\underline{i}$-matrix. The outer-fringe of the reduced $\underline{i}$-matrix is a $2(m-r)K+K$ component vector that we call the reduced $\underline{i}$-vector. The combination of the reduced p-vector and reduced $\underline{i}$-vector will be called the reduced code-vector.

Lemma 8: If the reduced $\underline{i}$-matrix is periodic of rank L, then the reduced p-vector is an output segment of an L-stage nonsingular linear FSR uniquely determined by the reduced $\underline{i}$-matrix. In particular,

$$p_j = \sum_{g=1}^{L} c_g p_{j-g} \quad (c_L = 1) \qquad j = r+L, r+L+L, \ldots, m-r \tag{25}$$

where c_g, $g = 1, 2, \ldots, L$, are the FSR connections uniquely determined by the reduced $\underline{i}$-matrix.

Proof: From (13) we see that the digits in each column of the reduced $\underline{i}$-matrix satisfy the recursion (25). But (24) shows that the reduced p-vector is always a linear combination of these columns and hence also satisfies the recursion (25).

We are finally in a position to tie all the preceding results together so as to obtain a Gilbert bound on d_{DD}.

We begin by noting that for $r \leq \Delta(m+1)$, where Δ, $0 < \Delta < \frac{1}{3}$, will be chosen later, if the reduced p-vector has fractional weight δ_p, then the entire code-vector has fractional weight δ' satisfying

$$\delta' \geq \frac{m-2r+1}{n_{DD}} \delta_p > \frac{1-2\Delta}{2K+1} \delta_p . \tag{26}$$

Similarly, if the reduced $\underline{i}$-vector has fractional weight δ_i, then

$$\delta' \geq \frac{2(m-r)K+K}{n_{DD}} \delta_i > (1-2\Delta)\frac{2K}{2K+1}\delta_i \qquad (27)$$

where the last inequality requires the proviso

$$m \geq \frac{1-2\Delta}{\Delta}$$

and henceforth we assume that we are considering only m sufficiently large to satisfy this inequality.

For a given δ, we wish to demonstrate the existence of a code such that $d_{DD} \geq \delta n_{DD}$. We begin by choosing

$$\delta_i = \frac{2K+1}{2K}\frac{1}{1-2\Delta}\delta < \frac{1}{2} \qquad (28)$$

and

$$\delta_p = \frac{2K+1}{1-2\Delta}\delta < \frac{1}{2} . \qquad (29)$$

We next divide the set of all possible code-vectors having $\underline{i}_0 \neq \underline{0}$ and fractional weight δ or less into two sets S_1 and S_2 defined as follows. S_1 contains only those code-vectors such that the $\underline{i}$-matrix has rank r satisfying $r \geq \Delta(m+1)$ and S_2 contains those for which the $\underline{i}$-matrix has rank r, $r < \Delta(m+1)$.

First consider the set S_1. S_1 cannot contain more than all of the code vectors of fractional weight δ or less, and each vector in S_1 appears in a fraction at most $2^{-(m+1)\Delta}$ of all codes. Hence the fraction F_1 of codes which contain any vector in S_1 satisfies

$$F_1 \leq \sum_{j=0}^{[\delta n_{DD}]} \binom{n_{DD}}{j} 2^{-(m+1)\Delta} \leq 2^{-n_{DD}\{\frac{\Delta}{2K+1} - H(\delta)\}} \qquad (30)$$

where here and hereafter we use [ ] to indicate the integer part of the enclosed number.

The consideration of set S_2 becomes considerably more interesting. From (26) and (27) we conclude that any vector in S_2 must have <u>both</u> fractional weight δ_i or less in its reduced $\underline{i}$-vector <u>and</u> fractional weight δ_p or less in its reduced p-vector. Hence, the number of distinct reduced code-vectors found within the vectors in S_2 such that the reduced $\underline{i}$-matrix has some given rank L is less than

$$2^{6KLH(\delta_i)} \; 2^{3LH(\delta_p)} = 2^{6KLH(\delta_i)+\,3LH(\delta_p)}$$

which follows from the facts that lemma 7 gives the first factor as bounding the number of reduced $\underline{i}$-vectors to be considered whereas lemmas 6 and 8 give the second factor as bounding the number of p-vectors to be considered with any given $\underline{i}$-vector. Note also that the reduced $\underline{i}$-vector is a non-zero output segment from a KL-stage non-singular linear FSR and hence must have at least one non-zero digit every KL digits which requires that it have fractional weight exceeding $\frac{1}{K2L}$. Thus S_2 contains no reduced $\underline{i}$-vector such that $L \leq \frac{1}{2K\delta_i}$. But the fraction of codes containing any reduced code-vector such that the reduced $\underline{i}$-vector in (24) has rank L is at most 2^{-L}. We conclude then that the fraction F_2 of codes containing any code-vector in S_2 satisfies

$$F_2 < \sum_{L=[\frac{1}{2\delta_i K}+1]}^{\infty} 2^{6KLH(\delta_i)+\,3LH(\delta_p)-L} \qquad (31)$$

With the aid of (28) and (29) and from the convexity of the entropy function, we obtain

$$F_2 < \sum_{L=[\frac{1-2\Delta}{2K+1}\frac{1}{\delta}+1]}^{\infty} 2^{-L\{1-6\frac{2K+1}{1-2\Delta}H(\delta)\}}$$

which upon summing of the geometric series yields

$$F_2 < 2^{-\frac{6}{\delta}\{\frac{1-2\Delta}{6(2K+1)}-H(\delta)\}} \qquad (32)$$

provided that

$$H(\delta) < \frac{1}{6}\frac{1-2\Delta}{2K+1} . \qquad (33)$$

Combining (30) and (32), under the proviso of (33), we find that the fraction of codes containing any element of S_1 or S_2 is at no

$$F_1 + F_2 < 2^{-n_{DD}\{\frac{\Delta}{2K+1} - H(\delta)\}} + 2^{-\frac{6}{\delta}\{\frac{1-2\Delta}{6(2K+1)} - H(\delta)\}} . \quad (34)$$

We now exercise the free choice that we have reserved and choose $\Delta = \frac{1}{6}$. (34) then becomes

$$F_1 + F_2 < 2^{-n_{DD}\{\frac{1}{6(2K+1)} - H(\delta)\}} + 2^{-\frac{6}{\delta}\{\frac{1}{9(2K+1)} - H(\delta)\}} . \quad (35)$$

We next choose δ to satisfy

$$H(\delta) < \frac{1}{10}\,\frac{1}{2K+1} \quad (36)$$

which we note is consistent with our proviso (33) and is also sufficient to guarantee that the first term in (35) vanishes as n_{DD} gets large. It remains to show that the second term in (35) is less than 1 . To see this we note that this term has its maximum value when $K = 1$ and (36) holds with equality in which case the term can be evaluated to be

$$2^{-\frac{6}{.0035}\{\frac{1}{27} - \frac{1}{30}\}} < 2^{-6} .$$

Hence, whenever (36) is satisfied, not all codes contain code vectors with $\underline{i}_0 \neq \underline{0}$ and fractional weight δ or less. We conclude that there exists as least one code with definite-decoding minimum distance d_{DD} satisfying

$$H(\frac{d_{DD}}{n_{DD}}) \geq \frac{1}{10}\,\frac{1}{2K+1}$$

for every n_{DD} sufficiently large. We state this result as:

Theorem 4: For $N = K + 1$ (and hence $R = \frac{K}{K+1}$), and for all n_{DD} sufficiently large, there exists at least one convolutional code such that

$$H(\frac{d_{DD}}{n_{DD}}) \geq \frac{1}{10}\,\frac{1}{2K+1} = \frac{1}{10}\,\frac{1-R}{1+R} \quad (37)$$

Theorem 4 provides our long-sought Gilbert bound for the special case when $N = K + 1$. We now sketch the manner in which this bound can be extended to arbitrary $N > K$. In the general case, there are $N-K$ p-vectors, each of which, say the h-th, satisfies (9) with $\underline{G}_j$ interpreted as the h-th row of the matrix G_j, $h = 1, 2, \ldots, N-K$. Thus each of these reduced p-vectors is an output sequence of the same linear FSR and hence the number of distinct reduced code-vectors in S_2 is less than $2^{6KLH(\delta_i) + 3(N-K)LH(\delta_p)}$. Equations (28) and (29) are now replaced by $\delta_i = \frac{N+K}{2K} \frac{1}{1-2\Delta} \delta$ and $\delta_p = \frac{N+K}{N-K} \frac{1}{1-2\Delta} \delta$. The other arguments go through virtually unchanged and result in:

Theorem 5: For any $N > K$ and for all n_{DD} sufficiently large, there exist convolutional codes of rate $R = \frac{K}{N}$ and definite-decoding minimum distance d_{DD} such that

$$H\left(\frac{d_{DD}}{n_{DD}}\right) \geq \frac{1}{10} \frac{1-R}{1+R} \quad . \tag{38}$$

4. Remarks

Robinson [2] has given what he calls a 'Gilbert bound' on d_{DD}, but this bound is not asymptotically useful since it shows d_{DD} growing less than linearly with n_{DD} for large n_{DD}. Wagner [11] has obtained an asymptotically useful bound on d_{DD} for a class of time-varying codes, viz. codes such that G_j in (1) is a periodic function of u. Wagner also used a different, and less natural, definition of the definite-decoding constraint length from that employed herein and his resultant bound was useful only for $R < \frac{1}{2}$. For Wagner's codes, but using our definition of constraint length, Morrissey and Costello [12] have recently obtained the bound

$$H\left(\frac{d_{DD}}{n_{DD}}\right) \geq \frac{1-R}{1+R} \tag{39}$$

for all n_{DD} sufficiently large. Time-varying codes are an artifice to avoid the rank problems encountered with ordinary convolutional codes that had to be surmounted in this paper, but appear to be of little practical interest due to the increased instrumentation complexity. We conjecture that tighter bounding arguments, particularly in our lemma 5 which is especially crude, can eventually do away with the additional factor of ten in (38) compared to (39). We could have improved this factor somewhat in the present instance, but only at the expense of complicating several proofs beyond what any reader could endure. We have settled for obtaining what we believe is the functional form of the tightest possible bound without concerning ourselves overly about the constant multiplier.

Lemmas 5 through 7 were proved some time ago by the author and used by Kolor [13] to obtain what we believe is the first asymptotically useful bound on d_{DD} for ordinary convolutional codes. Kolor restricted himself to the special case $K = 1$, $N = 2$. It is difficult to compare the $K = 1$ case in theorem 3 to Kolor's result since Kolor quite sensibly ignored the 'integer part' difficulties which to overcome rigorously caused our lemma 5 to be a very loose bound. Kolor's major result was a decomposition theorem for parasymmetric matrices (matrices of the form (10) with $K = 1$) which is essentially embodied in our theorem 3. In most respects, the material in section 3 is a generalization and simplification of the method used by Kolor for $K = 1$ and $N = 2$, as well as an attempt to put the theory in a rigorous framework.

Finally, it should be mentioned that Robinson [14] has proved an upper bound on d_{FD} that is asymptotically the same as the bound in section 2 and also reduces to the Plotkin block coding bound for $m = 0$. In the nonasymptotic case, for small $N - K$, the bound in section 2 is generally superior to Robinson's bound, but is inferior in general when $N - K$ is large. The virtue of the bound in section 2 is its conceptual simplicity and ease of derivation as compared to Robinson's bound.

REFERENCES

[1] A. D. Wyner, "On the Equivalence of Two Convolution Code Definitions," IEEE Trans. on Inf. Th., IT-11, pp. 600-602, October 1965.

[2] J. P. Robinson, "Error Propagation and Definite Decoding of Convolutional Codes," IEEE Trans. on Inf. Th., IT-14, pp. 121-128, January 1968.

[3] W. W. Peterson, Error-Correcting Codes, M. I. T. Press and Wiley, pp. 48-50, 1961.

[4] D. M. Jones, Private Communication, RCA Missile Electronics and Control Division, Burlington, Mass., 1962.

[5] S. Lin and H. Lyne, "Some Results on Binary Convolutional Code Generators," IEEE Trans. on Inf. Th., IT-13, pp. 134-139, January 1967.

[6] W. C. Wilder, "Extensions of the Plotkin Bound," Course VI S. M. Thesis, M. I. T., Cambridge, Mass., August 1967.

[7] J. J. Bussgang, "Some Properties of Binary Convolutional Code Generators," IEEE Trans. on Inf. Th., IT-11, pp. 90-100, January 1965.

[8] J. M. Wozencraft and B. Reiffen, Sequential Decoding, M. I. T. Press and Wiley, (see appendix), 1961.

[9] J. L. Massey, Threshold Decoding, M. I. T. Press, pp. 15-17, 1963.

[10] J. L. Massey, "Shift-Register Synthesis and BCH Decoding," to appear in IEEE Trans. on Inf. Th.

[11] T. J. Wagner, "A Gilbert Bound for Periodic Binary Convolutional Codes," to appear in IEEE Trans. on Inf. Th.

[12] T. Morissey and D. Costello, Private Communication, Univ. of Notre Dame, Notre Dame, Ind., 1968.

[13] R. W. Kolor, "A Gilbert Bound for Convolutional Codes," Course VI S. M. Thesis, M. I. T., Cambridge, Mass., August 1967.

[14] J. P. Robinson, "An Upper Bound to the Minimum Distance of a Convolutional Code," IEEE Trans. on Inf. Th., IT-11, pp. 567-571, October 1965.

This work was supported in part by the National Aeronautics and Space Administration (NASA Grant NGR 15-004-026 to the Univ. of Notre Dame) under liaison with the Flight Data Systems Branch of the Goddard Space Flight Center, and in part by the National Aeronautics and Space Administration (~~Grant NsG-334~~) and the Joint Services Electronics Program ((Contract DA208-043-AMC-02536)E) at the Research Laboratory of Electronics, Mass. Inst. of Tech.

NGR 22-009-031

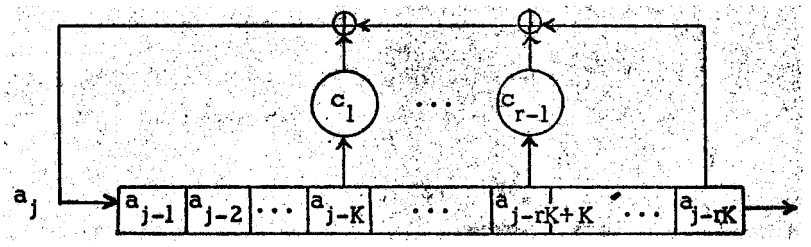

Figure 1. The rK-stage nonsingular linear feedback shift-register associated with a rank r periodic matrix.